



ADVANCED KEY MANAGEMENT

Stop Inventory Theft Through No-Nonsense
Key Control Policies and Training



Contents

03	FOREWORD WHAT IS KEY MANAGEMENT?
04	CHAPTER 01 BASIC KEY MANAGEMENT POLICIES
07	CHAPTER 02 ADVANCED KEY POLICIES FOR DEALERSHIPS
15	CHAPTER 03 KEY MANAGEMENT TRAINING FOR EMPLOYEES & MANAGERS
21	RESOURCES REFERENCES

FOREWORD

What is Key Management?

A quick online search for “key management” brings up two seemingly similar, but vastly different security processes.

The more prevalent definition involves cybersecurity protocols and best-password procedures. The digital management of code-breaking “keys” keeps interconnected systems and technologies safe from hackers.

Eyewitness recognizes the importance of internal cyber-key management. However, when we talk about “key management,” we mean something simpler and more tangible.

For our dealership clients, key management—also known as “**key control**”—is the **management of physical keys—both for the vehicles they sell and the buildings in which they operate**—to ensure the security of on-site assets and buildings.



A good key management policy or key control system involves both policies and security solutions





Basic Key Management Policies

If a business wants to maintain basic security within its walls, it must know to whom it distributes which keys, and in what circumstances.

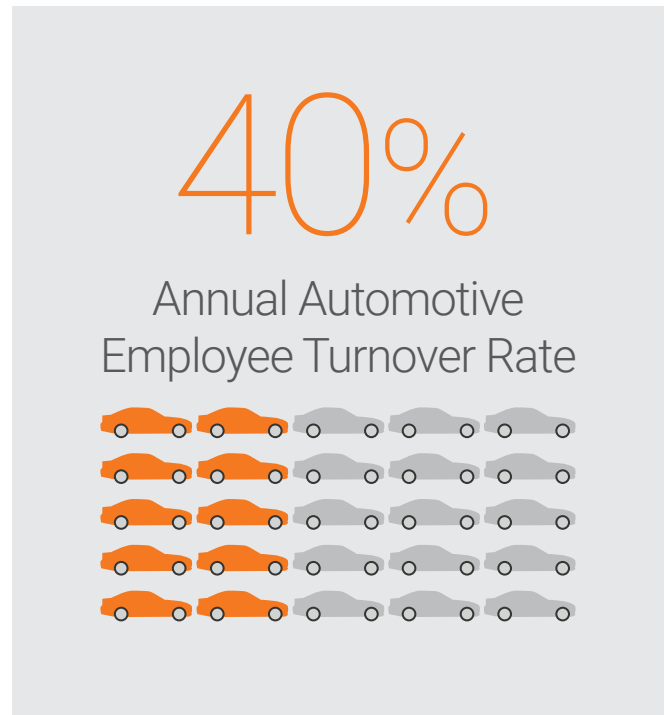
Management should also work out a process for what to do if a key is lost and stolen—before a key is misplaced—so panicked decisions don't make a bad situation worse.



Start with an audit: Do you know where your keys are?

If you don't already have written key management policies mapped out, there's no time like the present to start! Here's a quick checklist to get you going:

- ☐ Determine how many locked doors and storage facilities are on your property. Then, list which keys go to which doors—and who currently possesses those keys, as well as any potential copies of them.
- ☐ Consider which areas are especially “risky,” or require extra security and thus restricted access. Some possible restricted locked areas may be:
 - Gates onto and off the property
 - IT closet, which contains your servers and other hardware
 - Spare parts and equipment storage
 - Finance & Insurance (F&I) offices
 - Wherever inventory keys and car titles are stored
 - Computers with access to sensitive business and customer information
 - Retail merchandise storage areas
- ☐ Compare your list of locked locations, risk assessments, and available keys with your list of employees to determine who needs access to which areas for their everyday duties.
 - If someone only needs to access an area once a quarter, then they probably shouldn't permanently possess that area key. Consider setting up a “sign out” policy for specialty area keys with the central office. That way, people grab keys only when needed.
- ☐ Create a “lost key” protocol, as well as a procedure for key return during dismissal or resignations. With the annual automotive industry turnover rate at 40% in 2015 (67% for sales consultants), knowing how you ensure company property is returned without unauthorized copying is essential to maintaining security.¹



Physical Key Storage Solutions

If you're looking for ways to help mitigate loss due to poor key management, then it may be time to invest in professional key management and access control solutions. There are a wide range of physical security partners who can help you address various aspects of your key management problems.

Note that any vendors listed here have not been vetted by Eyewitness, and are provided for informational purposes only. We suggest doing extensive research before partnering with any security firm. After all, you're trusting them with the security and safety of your people and business—it's a huge responsibility, and one no business should take lightly.



Multiple Key Management


Useful for those who hold rings full of keys to important locations

 Morse Watchman's [Tamper-Proof KeyRings™](#)




Individual Key Control Solutions

Typically, these electronic locker-looking “key cabinets” automatically track who takes which keys, and when. Sophisticated models can even drill down to user-level permissions. (For example, you could make it so that only the GM and the IT Director could take out the IT closet key.)

 KeyTracer's [Key Cabinets](#)

 Morse Watchman's [KeyWatcher®](#) key control locker

 Morse Watchman's [KeyBank®](#) key control locker

 Security Key Systems' [Cobra Key Management System](#) as a mechanical—rather than electronic—solution to key storage



Advanced Key Policies for Dealerships

While the basic key control policies are a great place to start your key management strategy, you shouldn't stop there—especially if you want to prevent test drive theft and fake key swaps.

And, these events aren't just us being overly cautious—they happen to dealerships across the country every day:

In March 2017, for example, a Kansas salesperson found herself abandoned in a parking lot during a test drive² after a “customer” tripped her while switching places, driving off without her. [SEE MORE >](#)

In Oklahoma City, a thief gave the salesperson a fake key fob after the test drive,³ returning later to take the vehicle without anyone the wiser. [SEE MORE >](#)



Key Management Strategies for Inventory

Automotive dealerships have an additional unique key management issue: Organizing and protecting keys of their cars. Millions of dollars' worth of inventory-on-wheels can be quickly and quietly stolen if a dealership doesn't sufficiently protect their car keys from theft.

Written and enforced key management policies can greatly decrease the possibility of key theft without costing a dime. Some common sense suggestions include:



DO Keep all car keys in a central, restricted-access location with some sort of record of who took which keys, when, and the time of their return.



DO periodically audit the key storage records to identify trends of compromising behavior and possible missing inventory.



NEVER allow employees to store car keys at their desks or in their briefcases and purses for any substantial length of time.

- This is especially important if potential customers wait at salespeople's desks for unsupervised periods.

BROWN AUTOMOTIVE KEY SIGN-OUT SHEET

Key Number	Employee	Date	Time-Out	Time-In
#030417	TONY STEPHENSON	9/15/17	9:48am	10:50am
#827503	Sarah Filson	9/15/17	11:05am	2:45pm
#559801	TONY STEPHENSON	9/15/17	2:20pm	4:16pm
#634016	Matthew Smith	9/15/17	3:06pm	3:52pm
#301429	Jen Cannon	9/15/17	4:21pm	5:10pm



Reviewing storage records is a great way to prevent loss and compromising behavior

Prevent test drive thefts and fake key swaps

The thefts mentioned earlier in Kansas and Oklahoma don't have to happen to your dealership. We've got three practices you can adopt to stop these thefts before they ever happen.

1. Add a dealership-specific keychain to all vehicles

Keychains are some of the least expensive pieces of marketing "swag" available, printable in dozens of colors and shapes for literally pennies apiece. It's relevant piece of physical marketing collateral your dealership may want to consider—especially when used as an anti-theft device.

Blank branded key fobs are incredibly easy to purchase online at digital auctions or marketplaces. Key swap thieves don't need the fob to work, of course—just look enough like the

physical key at a casual glance so dealership employees are fooled into accepting it in place of the real one.

However, if every dealership key ring also holds a dealership-specific keychain—**one that the dealership has especially designed and ordered that a thief couldn't buy online**—then it makes key fob swaps much harder.

If you'd like to try something like this at your dealership, order two separate lots of custom keychains. Design one keychain lot specifically for public distribution to customers and walk-ins as marketing collateral. Then, design a separate—and visually distinctive—keychain to be used only for unsold vehicles, and which are never distributed outside the dealership to non-employees.



Consider using one style of keychain for giveaways, and another that is specific to avoid potential key swaps



2. Never allow a customer to hold a car key fob.

Selling a car can be a bit like selling wedding dresses: If you place a customer within the car or the gown, they're much more likely to purchase something they originally considered out of their price range.

Allowing a customer to hold the smart key fob—to feel in control and get a taste of life possessing this beautiful and expensive item—can help sell the vehicle. However, letting a customer touch and handle a car key is riskier than encouraging a bride to don a veil, since a key fob can be hidden more easily than a nine-yard swath of lace and chiffon.

Even if a dealership lets the customer handle a key while reviewing paperwork, it's easy to distract the salesperson for a moment with payment queries and other details that require their momentary departure. That's more than enough time for a slick thief to perform a key swap.

So, reconsider any sales tactics that allow a customer to ever hold, use, or pocket a smart car key at any time during the transactional process. Ask yourself: Does that one sales tactic sell enough vehicles to make up for the potential loss of one car (or many cars) due to smart key fob swaps?

3. Learn sleight-of-hand to deter pickpockets.

So, let's say that your dealership uses branded keychains on all unsold vehicle key rings, and enforces a key management policy that prohibits potential customers from handling keys. Great! That's most of the battle.

But pickpockets do still exist, even in 2017. A desperate, clever thief may still go "back to basics" in a manner of speaking, and physically pick the pocket of a salesperson, overcoming those proactive key management policies altogether.



Sales Training Exercise

For an interesting (and fun!) exercise, spend an hour teaching your employees how to spot sleight-of-hand tricks and foil pickpockets at their own game. Here are some quick suggestions to start you off:

- **Be aware of your personal space bubble.** Pickpockets and other thieves can press against you in such a way, as to leave a lingering pressure sensation—making you think you still have the item when you really don't.⁴
- **Keep keys in your front pocket,** not a back one. You're more likely to sense invasions of personal space and theft in front of you than in back.
- **Keep smart keys in a zippered pouch** or otherwise secured pocket/purse whenever possible.
- **Avoid holding keys and other valuables.** The more often you physically handle a small valuable, the more likely you are to set it down someplace insecure—completely bypassing the need to pick an actual pocket.

How Criminals Use Key Fob Technology

Cars these days are essentially two-ton computers on wheels, most obviously through advances in key technology. Remember the days you had to put a metal key to turn the ignition? Now, you just press a power button on the dashboard.

That said, cars operating primarily from wireless key fobs are vulnerable to advanced theft in two specific ways.

1. Criminals can “boost the signal” of your key fobs.

Cars with smart keys and key fobs typically rely on weak radio signals to detect key proximity. A smart key fob contains a small radio pulse generator within the key's housing, broadcasting its security code within a limited area. (Think less than two feet.)

That radio signal is picked up by the car's antennae, which is constantly listening for the matching key security code. If the car can sense the smart key's security code signal, it assumes the key itself is nearby and allows the holder to unlock and start the car.

While the original signal from the key fob is relatively weak, it's simple to “boost” that signal.

Using an ordinary power amplifier, criminals trick the vehicle into receiving the key's security code signal—even if the key is hundreds of feet away.

Once the car is turned on, “thinking” the key is inside, the criminal then drives away.

Eventually, the power amplifier will no longer be able to boost the key's signal, as the thief drives away from the smart key. That's not much of a problem for the criminal, since the car doesn't shut down its engine if the key is no longer sensed. It simply alerts the driver that the key is no longer sensed—but they already know the key isn't present.



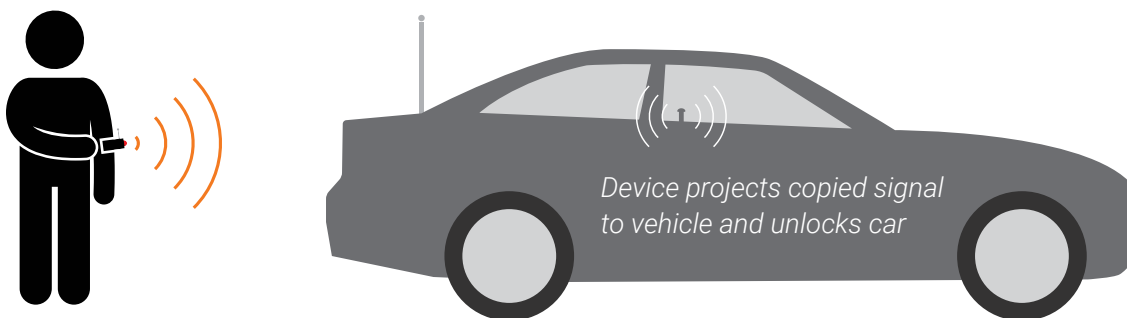
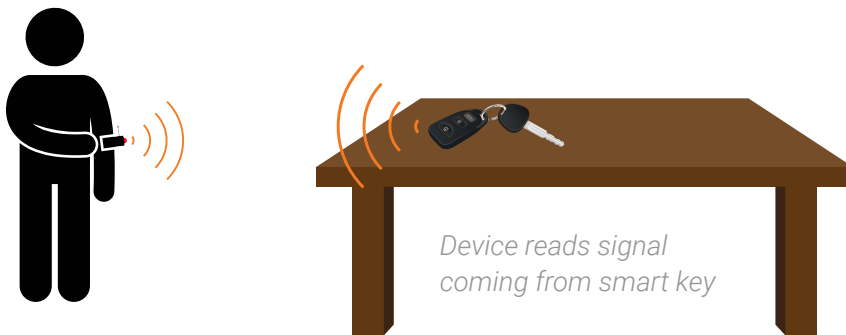
2. Criminals can “copy” your key fob radio signal security codes.

This process is a bit more involved, but still a comparatively economical way for ne’er-do-wells to steal your vehicles. It involves two pieces of equipment: One to copy the key’s radio signal, and a second to mimic it.

In December 2016, the National Insurance Crime Bureau announced that it had **tested a “mystery device” that copied and replicated a vehicle’s key fob signal, allowing thieves to unlock and steal these cars.**⁵ The signal could be received from up to 10 feet away, so this process also doesn’t require hands-on access to a smart key fob.

The device the NICB obtained was from an overseas manufacturer who produces this and similar technologies to help manufacturers evaluate vulnerabilities within the vehicles. So, this device isn’t exactly common on the streets.

Still, it’s a technology that exists and could become available on a more widespread basis as more criminals become technologically savvy. That’s why we suggest taking special precautions to prevent your cars from being stolen with hijacked smart key technology.



Prevent Smart Key Thefts with Faraday Cages

So, smart keys and keyless entry systems can leave a gaping security risk on your car lot, which criminals can easily exploit.

If you're aware of the problem, though, you can plug the security hole through a most unlikely source: Faraday cages.

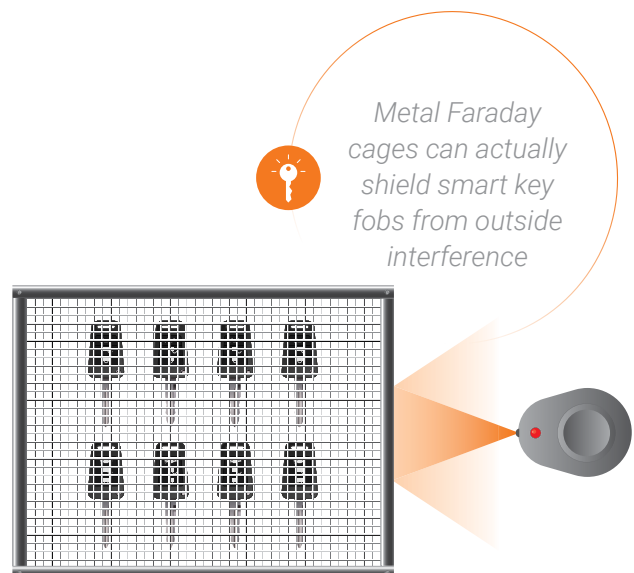
What Are Faraday Cages?

A “Faraday cage” (or “Faraday shield,” as it’s sometimes known) sounds like something from a weird science-fiction dungeon, but it’s a real device created in 1836 by inventor Michael Faraday.

He discovered that by running an excessive electrical charge around a metal container, the charge will linger on the outside to insulate whatever was contained within the skin. (Faraday based his cage on the work of an earlier inventor: Benjamin Franklin.)

Today, Faraday cages are used to shield important data from outside interference—particularly from external radio signals. You’ve probably seen the special “metal wallets” or metal-lined purses touted for their ability to prevent hackers from stealing credit card information from embedded chips. These products are based on a Faraday cage concept.

You can use Faraday cages at your dealership to protect your key fobs from criminals’ signal boosting or copying efforts. Inside a Faraday cage, the smart keys’ radio signals would be blocked from leaving the cage due to the current, and no signal could reach into the cage to copy the keys’ security codes.



Purchase portable Faraday shields for everyday use.

Since your dealership's employees need to use smart keys on a regular basis on test drives with clients, you need a portable security solution to prevent your keys' signals from being copied on the go.

Several manufacturers create special Faraday cage-based bags and products to shield important items from intrusive radio signals. Consider investing in a Faraday-cage bag for each employee who handles keys during the day.

Smart keys and key fobs should never be left out on a desk or in a drawer without being protected by a Faraday shield. Otherwise, their signals are exposed to any person with a signal hacker in the vicinity.



Portable Faraday pouches can be given to every employee authorized to carry smart keys.



Create a Faraday cage-based storage solution—an electronic key safe—for overnight key storage.

Microwaves and refrigerators are out for key fob storage, so you'll have to invest in a "proper" Faraday cage solution for your primary key storage.

You can always buy metal safes with built-in Faraday cage currents, which aren't overly expensive. They're available from several safe manufacturers online and in-person.

There are also some interesting DIY kits and solutions online to be found, though we can't speak to their ease or efficacy. (If anyone's ever built a Faraday cage, we'd love to know!)

At the very least, **don't store your inventory smart keys in a wooden container or cabinet.** The thick metal walls of a generic safe also interfere with radio signals to help deter signal-thieves, though it's not as secure as a true Faraday cage. In this case, a metal filing cabinet is better than nothing—even if it's less attractive.

Your dealership may already have been impacted by "smart thieves" boosting key signals for their own nefarious purposes, and you'd never know. After all, it's a relatively clean mode of entry, leaving behind no evidence for you or the police to examine. Take a proactive approach toward your security and insulate your dealership against theft—literally!



If getting a Faraday cage is not an option, we still recommend storing keys in a metal container, like a file cabinet.





Key Management Training for Employees & Managers

Writing an effective key control policy is (comparatively) easy. Enforcing it is the hard part, especially when you've got high employee turnover—and that turnover rate makes key management even more important!

To keep things simple for employees old and new, we've put together five **"key commandments."** These rules outline the foundation strategies required in every effective key management policy.

Management and staff will see these rules differently—managers from a strategic and enforcement perspective, and staff on a day-to-day level. Overall, these key commandments offer a great baseline for everyone in your dealership to use.



Learn how both employees and management can successfully execute these commandments.

5

Key Commandments

- I. Who Has Which Key, When
- II. Keep Keys in Sight or Storage
- III. Lock Up Before You Take Off
- IV. Keep One Key at a Time
- V. Replace Locks for Every Missing Key

I Who Has Which Key, When

EMPLOYEES

It's vital that employees know where their business keys—both permanently assigned and borrowed—are at all times. (After all, they can't do their jobs if they can't access the building!) This rule is relatively easy for them to keep, then, with two small exceptions.

1. **Sign Out Policies:** The company's sign-out policy for borrowing keys must be adhered to all the time. No grabbing a key from a coworker who's done with it—the office must know who has a key all the time. Yes, it's annoying to go to the office and re-sign out the key. However, these sorts of proactive key protocols protect everyone—including the employee—from key-related loss and repercussions.
2. **Missing Keys:** Key loss happens all the time, accidentally and nefariously. Employees must feel empowered to approach management to report missing keys if the building and its inventory is to remain secure.

MANAGERS

Managers should conduct biannual key audits to determine:

- **Which doors, lockers, and areas have locks** (and which areas need them)
- **How many keys exist** for a given lock
- **The location of every key**, whether it's been assigned to an individual or to the office for sign-out borrowing
- **Who is authorized to access which areas**, and if they have the keys necessary to perform their daily duties

Furthermore, sign-out policies should be instituted to track who signs out keys, when.

If the company has a keyless access control system installed, a key audit is easily accomplished in a matter of key strokes (pun slightly intended). Plus, access control systems like Eyewitness Surveillance's automatically track who tries to access which door and time stamps it, creating an auditable log of activity for every secured location in your business.

Billy Dine



II Keep Keys In Sight or Storage

EMPLOYEES

Keys—especially borrowed keys to sensitive areas or expensive inventory—should never leave the sight of an employee.

If a customer goes on a test drive, a salesperson should be with them to ensure the key will not be stolen. Never should a customer be allowed to walk away alone with a key the company owns, no matter how compelling the reason. (“I want to know what the car sounds like with the clicker” is not an acceptable reason—otherwise, you’ll fall for the same key swap scheme an Ohio dealership did in May 2017.)⁶

MANAGERS

This rule can bump against some dealership’s standard selling practice of solo test drives to increase a customer’s emotional attachment to a given vehicle prior to purchase. (And indeed, many test drive thefts would have been avoided, if an employee had accompanied the drive.)

Weigh the value of the solo test drive against the potential loss of inventory, and make your determination that way.

It’s not always a black-or-white decision, either. You could always implement a policy of quick background checks, using a customer’s provided license and insurance card. Should the check return red flags, insist on an accompanied test drive. If it comes back clear, then consider allowing a solo drive in exchange for some valuable piece of collateral or guarantee.



III Lock Up Before You Take Off

EMPLOYEES

It's amazing how many lockable doors, areas, and storage containers there are in a car dealership—and all of them must be secured before the building is considered safe from intruders.

So, even if an employee's personal area is secured—with all extra keys returned to the office and personal belongings locked away—the overall building's security may be compromised if even one small door or window lock is forgotten. Go over every lock and door before leaving for the night, to ensure the building's complete safety.

This rule has daytime application, too. Don't prop open doors for easy access, or allow unrecognized people to "piggyback" into the building behind folks who swiped their card. Also, don't hide keys in "clever" places in unlocked vehicles for easy future access.⁷ You're giving criminals easy access, too.

MANAGERS

A physical closing checklist—in addition to verbal instructions or reminders—will help employees remember all the steps required to closing the business for the night. Eventually, the pattern will become rote habit, but new employees in the middle of their onboarding training should find written instructions helpful.

Plus, it offers employees a concrete rubric against which their performance can be judged. (Was the service bay entrance left unlocked? Well, it's on the checklist—no excuse to forget!) Employees will know exactly what they're responsible for, so it's no surprise when they're evaluated on it come performance review time.



EYEWITNESS IN ACTION

Recently, our tactical command center noticed a client's main showcase doors kept flying open in the middle of the night for no apparent reason. Because we were watching over the facility, no theft or intrusion occurred, but it was still a gaping security vulnerability for our client. We reported it to our client, who couldn't figure out why doors were unlocked after regular closing procedures.

As it turns out, an employee was forgetting to insert a center pole in the bay doors that locked them at night. He simply closed the doors and headed back to his car, forgetting the pole altogether. The owner verbally corrected him on the spot, and the doors haven't opened since.

Keeping an eye on even veteran staff—this salesman had been with this client for years!—will ensure your installed locks actually keep people out..

IV Keep One Key at a Time

EMPLOYEES

Staff should never have more than one “extra” key at any given time, beyond the keys they’ve been permanently issued. **Temporarily storing keys in desk drawers, pockets, or purses is an invitation for criminals to go snooping.**

Every time an employee needs a new key, they must go to the office to return the old key (if any) and check out a new one. Don’t horde keys at your desk for mass return at the end of the day!

Also, employees should not hand a borrowed key to a coworker once they’re done with it. Their name is still recorded as the one in possession of the key. If that key is stolen or lost on the coworker’s watch, the first employee who signed out the key would be responsible for its loss (and any subsequent theft). Decrease personal liability by following key management sign out procedures!

MANAGERS

Employees will be more likely to adopt policies they view as cumbersome or annoying if managers also follow them. Don’t exempt yourself from this policy because you find it annoying. If you find yourself borrowing a building key frequently, then consider having one made for your permanent assignment. Otherwise, borrow it from the office. (Of course, those managers with access control systems can adjust keyholder permissions without requiring new keys to be cut or assigned.)

Also, conduct visual spot checks of employee desks and areas to see if keys are out in the open for anyone to take. Consider random desk inspections to check for key stashes in drawers. Don’t let this procedure slack during busy hours—it’s the difference between keeping your inventory and losing it.





Replace Locks for Every Missing Key

EMPLOYEES

Last but not least, we have the cardinal rule of key management: Locks only work if they're used—and if every key is accounted for. If a key is missing, then the lock to which it goes should be considered compromised.

We repeat: **If a key is missing, the lock is no longer secure.** Building, storage area, inventory—if its key is gone, then it is vulnerable to theft. Making a new key to replace the missing one only allows for access, not increased security.

Therefore, when keys are missing for longer than 72 hours, that lock must be replaced to ensure the security of the entire building.



MANAGERS

Replacing locks as often as employees lose them is astronomically expensive, but consider how much your business's materials are worth. Inventory, equipment, supplies, and customer information—you place every valuable at risk when the lock to a lost key is not replaced.

If you'd rather not manually replace locks and keys every time an employee loses one, though, there is a solution. Eyewitness's keyless access control system allows management to adjust keyholder permissions on the fly. **If someone loses their card or fob, you can erase that card or fob's permissions and assign a new one to the employee—without replacing the lock or anyone else's keys.**

So that's it! Five easy "key commandments" for employees and managers to follow. Let these five rules guide both your day-to-day operations, as well as your overall strategy for business safety and security.



REFERENCES

- ¹“Employee turnover costs dealers billions” by Amy Wilson / Automotive News <http://www.autonews.com/article/20170123/RETAIL06/301239850/employee-turnover-costs-dealers-billions>
- ²“Kansas Test Drive Trips Into a Theft” from The Eyewitness National Crime Alert for March 20, 2017 <http://www.eyewitnesssurveillance.com/eyewitness-national-crime-alert-march-20-2017/>
- ³“Man Gives Employee Fake Key Fob, Steals Dodge Charger” from The Eyewitness National Crime Alert for February 27, 2017 <http://www.eyewitnesssurveillance.com/eyewitness-national-crime-alert-february-27-2017/>
- ⁴“Revealed: The secret sleight of hand used by thieves to remove a watch from a victim’s wrist” by Victoria Moore <http://www.dailymail.co.uk/news/article-461840/Revealed-The-secret-sleight-hand-used-thieves-remove-watch-victims-wrist.html>
- ⁵“Your keyless ignition might not be theft-proof: Thieves Are Using ‘Mystery Devices’ to Steal Push-Button Ignition Equipped Cars” by John Irwin <http://autoweek.com/article/technology/your-keyless-ignition-might-not-be-theft-proof>
- ⁶“\$10,000 Reward for Key-Swapping Sneaks” from The Eyewitness National Crime Alert for May 22, 2017 <http://www.eyewitnesssurveillance.com/eyewitness-national-crime-alert-may-22-2017/>
- ⁷Advanced Key Management: 6 Terrible Car Key Hiding Spots by David Snyder <http://www.eyewitnesssurveillance.com/key-management-terrible-car-key-hiding-spots/>



If you'd like to talk more about what key management options would be best for your dealership—including keyless access control systems for all your dealership's sensitive areas—

CALL US toll-free at **800-518-3911** or
EMAIL info@eyewitnessmail.com for more information.

Because while any security is better than no security, some security companies work harder to protect your employees and your bottom line than others. We'd love the chance to prove that we're one of the "good ones."